IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE

CHERYL EAKINS,

Plaintiff,

vs. **Case No. _____**

CARRIER IQ, INC.

SERVE: National Registered Agents, Inc.
200 West Adams Street
Chicago, IL 60606

SAMSUNG TELECOMMUNICATIONS AMERICA, INC., SAMSUNG ELECTRONICS AMERICA, INC.

SERVE: CT CORPORATION SYSTEM
120 South Central Avenue
Clayton, MO 63105

And

SPRINT COMMUNCIATIONS COMPANY, L.P. d/b/a SPRINT NEXTEL or NEXTEL RETAIL STORES, L.L.C.,

Corporation Service Company
2908 Poston Ave.
Nashville, Tennessee 37203-1312 USA

Defendants.)

COMPLAINT FOR DAMAGES PURSUANT TO THE FEDERAL WIRETAP ACT AND THE COMPUTER FRAUD

Cheryl Eakins ("Plaintiff"), by her undersigned counsel, for herself and all others similarly situated, hereby commences the suit against Defendants Carrier IQ, Inc.

("Carrier IQ" or "Defendant"), Samsung Telecommunications America, Inc (Samsung) and Sprint Nextel, or Sprint Communications Company LLC (hereinafter referred to as "Sprint") for statutory, compensatory, punitive, equitable, injunctive, and declaratory relief. Plaintiff makes the following allegations based upon personal knowledge as to her own acts, and upon information and belief, as well as upon her attorneys' investigative efforts as to Carrier IQ's actions and misconduct, and alleges as follows:

PRELIMINARY STATEMENT

1. The lawsuit arises out of the undisclosed and unauthorized monitoring, recording, and transmission of the keystrokes, data sent and received, location, numbers dialed, message content, websites visited, encrypted web searches, and the private information of millions of mobile device users by Defendants. The information is extremely sensitive and private. AT&T and Apple Defendants acted through monitoring software designed and distributed by Carrier IQ. The software is intentionally concealed from mobile device users. Even if consumers are aware of the software, they cannot remove or deactivate it.

2. Plaintiff brings this lawsuit on her own behalf, as an individual user of mobile devices that operate the Carrier IQ software – and alleges that Defendants' conduct violates the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.* Plaintiff seeks actual damages, statutory damages, punitive damages, disgorgement and restitution, and attorneys' fees and costs.

PARTIES

1. Cheryl Eakins is a natural persons and citizens and resident of the State of Tennessee.

Is the owner of a cell phone manufactured by Defendant, Samsung. She is also a previous Samsung cell phone customer. At all times material herein, the Plaintiff was provided cellular service by Defendant, Sprint. Her phones have been provided to her with the IQ Agent or Carrier IQ software previously installed without her knowledge. She has used her phone for phone calls, to transmit text messages and send and receive data at all times material to this complaint.

2. All references to "Plaintiff(s)" throughout her Complaint are made on behalf of herself as an individual.

3. The amount in controversy in this action, as defined by 28 U.S.C. § 1332(d)(6), exceeds $5,000,000 exclusive of costs and interest.

4. Defendant, **Carrier IQ, Inc**. (hereinafter referred to as "CIQ") is a citizen of California as defined by 28 U.S.C. § 1332(c) with its principal place of business in California.

5. Defendants **Samsung** Telecommunications America, Inc., and Samsung Electronics America, Inc. (collectively referred to as "Samsung") are citizens of Texas and New Jersey, with their respective principle places of business in Texas and New Jersey. Defendant, **Sprint Communications Company, or Sprint Nextel,** is a Delaware Corporation, licensed to and doing business in the State of Tennessee. It may be served with process through its registered agent, the Corporation Service Company, 2908 Poston Ave., Nashville, TN 37203.

6. Defendants are residents of the Western District of Tennessee as they have ongoing and systematic contacts with residents of the Western District of Tennessee. Defendants

have, at all material times, conducted business in the Western District of Tennessee of Tennessee. Moreover, Defendants have sufficient minimum contacts with the State of Tennessee such that the assumption of jurisdiction will not offend traditional notions of fair play and substantial justice.

7. When reference in the Complaint is made to any act or omission of Defendants, it should be deemed to mean that the officers, directors, agents, employees, or representatives of Defendant committed or authorized such act or omission, or failed to adequately supervise or properly control or direct their employees while engaged in the management, direction, operation, or control of the affairs of Defendant, and did so while acting within the scope of their employment or agency.

FACTUAL ALLEGATIONS

7. Carrier IQ designs, develops, and markets software capable of tracking, recording, and transmitting electronic data to wireless service providers or the Carrier IQ customers ("Carrier IQ Software" or "rootkit software"). Carrier IQ refers to the Carrier IQ Software as the IQ Insight Experience Manager or as the IQ Agent.

8. The Carrier IQ Software is found on over 140 million smartphones and mobile devices.

9. Wireless carriers Sprint, AT&T, and T-Mobile acknowledge that they utilize the Carrier IQ Software.1 On December 1, 2011, Defendant Sprint confirmed that handsets on its network run Carrier IQ's Software and transmit information from it back to them. However, Defendant Sprint does not inform consumers how the information is used. It has caused the Carrier IQ software to be installed on its phones since 2006.

10. The Carrier IQ Software can be found on smartphones and mobile devices manufactured by HTC, Samsung, and others.

11. Once the Carrier IQ Software is installed on a smartphone, it surreptitiously runs in the background, capturing and logging the user's activities. The Carrier IQ Software functions by recording the user's key strokes and transmitting that data to a separate location that can be accessed by wireless service providers.

12. The Carrier IQ Software is a rootkit. A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators (consumers who own the mobile devices, including Plaintiff) by subverting standard operating system functionality or other applications.

13. The rootkit software records personal and private information, including:

a. When a user turns her or her phone on and off;

b. The phone numbers a users dials;

c. The contents of the text messages the user receives;

d. The URLs of the websites the user visits;

e. The contents of the user's online search queries; and

f. The user's location—even when the user has expressly denied permission for that information to be recorded.

14. Carrier IQ states on its website that it is the "leading provider of Mobile Service Intelligence Solutions to the Wireless Industry. As the only embedded analytics company to support millions of devices simultaneously, we give Wireless Carriers and Handset Manufacturers unprecedented insight into their customers' mobile experience."

15. Carrier IQ's website defines "Mobile Service Intelligence" as "the process of analyzing data from phones to give you a uniquely powerful insight into mobile service quality and user behavior."

16. At the direction of wireless carriers, mobile device manufacturers embedded the Carrier IQ Software in various models of smartphones and mobile devices. Consumers are not informed about the inclusion of the rootkit software on their smartphone at the time of purchase, nor at any other time.

17. In November 2011, Trevor Eckhart, a systems administrator and information technology expert in Connecticut, discovered the hidden rootkit software and posted about it (and the extensive data it captures) on her website, http://androidsecuritytest.com.

18. After Eckhart published the information he discovered on her website, Carrier IQ initially threatened him with litigation in an attempt to force him to take the information down. After public outcry – including a letter from Senator Al Franken demanding an explanation from Carrier IQ – Carrier IQ abandoned its effort to silence Eckhart.

19. In an interview with *Wired*, an online magazine, Andrew Coward, Carrier IQ's chief marketing officer, answered "probably yes" when asked whether Carrier IQ could read mobile users' text messages. Coward admitted that the data collected by the Carrier IQ Software is "a treasure trove" of "sensitive information."

20. Data logged by the rootkit software includes keystrokes. A keystroke is a character selected by the user on the user's keyboard. The means that every letter, number, and punctuation mark that a user enters on her or her smartphone keyboard is logged by the

rootkit software, including web addresses, emails, text messages, and user names and passwords (even when the website uses a secure (https) connection).

21. The Carrier IQ Software also monitors application usage.

22. Carrier IQ's website states that it "takes customer experience profiling to another level, enabling [the mobile service provider] to view experience data at any level of granularity from the entire population, to comparative groups, down to individual users, all at the touch of a button."

23. Carrier IQ advertises its software as possessing the ability to "[c]apture a vast array of experience data including screen transitions, button presses, service interactions and anomalies."

24. The Carrier IQ Software gathers the data from a person's mobile device and transmits it to either a wireless carrier's network or to the Carrier IQ facilities approved by the network.

25. The Carrier IQ Software cannot be turned off.

26. The Carrier IQ Software operates by listening for commands called "triggers." For example, a user opening an application on her or her smartphone can be a trigger for the Carrier IQ Software to record and transmit information.

27. What actions serve as triggers to the Carrier IQ Software is predetermined by Carrier IQ and the wireless service providers. At a minimum, these include every time the user: (1) presses a key on the phone; (2) changes physical locations; (3) taps the screen; and (4) accesses a webpage. Other actions can also trigger the Carrier IQ Software.

28. Once triggered, the Carrier IQ Software records certain information. The information is then sent to another location, called the Carrier IQ Portal, where the information is stored and organized.

29. At the Carrier IQ Portal, devices are displayed by individual phone equipment ID and subscriber ID. Portal administrators can organize the information and subdivide the data sets further depending on their needs.

30. Carrier IQ's own patent for the rootkit software states that it is a "method for collecting data at a server coupled to a communications network." The patent states that the data to be collected relates "to an end user's interaction with the device," and that the interaction is "the end user's pressing of keys on the device."

31. Carrier IQ's own marketing materials further show that the rootkit software transmits personal and private data to wireless service providers. The marketing material promotes the software stating the software:

a. Is able to "capture a vast array of experience data including screen transitions, button presses, service interactions and anomalies;"

b. Allows users to see "application and device feature usage, such as camera, music, messaging, browser, and tv;" and

c. Allows users to "[i]dentify exactly how customers interact with services and which ones they use. See which content they consume, even offline."

32. The Carrier IQ Software also degrades the performance of all mobile devices in which it is installed. The software is always operating and cannot be turned off. It uses system resources, thus slowing performance and decreasing battery life. As a result,

because of the Carrier IQ Software, Plaintiff is not receiving the optimal performance of the smartphones that she purchased, which are marketed in part based on their speed, performance, and battery life.

JURISDICTION AND VENUE

33. The Court has original jurisdiction pursuant to 28 U.S.C. § 1331 because Plaintiff brings claims arising under federal law based on Defendants' violations of the Stored Communications Act, 18 U.S.C. §§ 2702 and 2707; the Wiretap Act, 18 U.S.C. § 2510 *et seq.*; and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

34. Additionally, and in the alternative, the Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A). Thee is minimal diversity and the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

35. Venue is proper in the District of Minnesota because a substantial part of the events or omissions giving rise to the claims occurred in Minnesota, Plaintiff resides in Minnesota, and all Defendants regularly do business in and are subject to personal jurisdiction in Minnesota.

COUNT I

Electronic Communications Privacy Act – Stored Communications Act

18 U.S.C. §§ 2702, 2707

43. Plaintiff incorporates the allegations in each above numbered paragraph.

44. The Stored Communications Act prohibits an entity providing an electronic communication service or remote computing service from knowingly divulging the contents of a communication while in electronic storage. 18 U.S.C. § 2702(a)(1)-(2).

45. Defendants provide electronic communication services to the public. 18 U.S.C. § 2510(15).

46. Defendants provide remote computing services to the public. 18 U.S.C. § 2711(2).

47. The Carrier IQ Software tracked, gathered, stored, transferred, and removed keystroke data – including data communications, phone calls, and voice messages – from Plaintiff's mobile devices without her knowledge.

48. Defendants intentionally and knowingly divulged to third parties the contents of stored keystroke data taken from Plaintiff's mobile devices while the keystroke data was placed in storage. Defendants knowingly divulged the contents of Plaintiff's communications, records and/or other information pertaining to them to third parties in violation of 18 U.S.C. § 2702(a).

49. Plaintiff has suffered actual damages as a result of Defendants' violations of 18 U.S.C. § 2702, including paying service and other fees and losing functionality and performance of their mobile devices, failing to receive the benefits of products impliedly represented to be secure with respect to personal information, and suffering the disclosure of their private information.

50. Pursuant to 18 U.S.C. § 2707, Plaintiff seeks on behalf of herself preliminary and permanent injunctive, declaratory, and equitable relief as may be appropriate; statutory damages, actual damages, and disgorgement of any profits made by Defendants as a result of the violation, in an amount no less than $1,000; punitive damages; and reasonable attorneys' fees and litigation costs.

COUNT II

Electronic Communications Privacy Act – Wiretap Act

18 U.S.C. § 2510 *et seq.*

51. Plaintiff incorporates the allegations in each above numbered paragraph.

52. The Wiretap Act, 18 U.S.C. § 2510 *et seq.*, regulates the interception and disclosure of wire, oral, and electronic communications.

53. Electronic communications are "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by" any electronic communications system that affects interstate or foreign commerce. 18 U.S.C. § 2510(12).

54. Electronic communications systems include "any computer facilities or related electronic equipment for the electronic storage of" electronic or other communications. 18 U.S.C. § 2510(14).

55. Through the Carrier IQ Software and any implementing or ancillary software exclusively controlled by Defendants, Defendants have intentionally intercepted, endeavored to intercept, and/or procured others to intercept wire, oral, and/or electronic communications without the knowledge, consent or authorization of Plaintiff, in violation of 18 U.S.C. § 2511(1)(a).

56. Through the Carrier IQ Software and any implementing or ancillary software exclusively controlled by Defendants, Defendants have intentionally disclosed and endeavored to disclose to third parties the contents of wire, oral, and electronic communications while knowing or having reason to know that information was obtained

through the unlawful interception of the communications, in violation of 18 U.S.C. § 2511(1)(c).

57. Through the Carrier IQ Software and any implementing or ancillary software exclusively controlled by Defendants, Defendants have intentionally used and endeavored to use the contents of wire, oral and electronic communications while knowing or having reason to know that information was obtained through the unlawful interception of the communications, in violation of 18 U.S.C. § 2511(1)(d).

58. As a result of Defendants' violations of the Wiretap Act, Plaintiff suffered harm and injury, including the interception and transmission of private and personal communications and the degraded performance level of their mobile devices.

59. Recovery of civil damages is authorized because Plaintiff are "person[s] whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of" the Wiretap Act. 18 U.S.C. § 2520(a).

60. Plaintiff, pursuant to 18 U.S.C. § 2520, are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 per day for each day of violation, actual and punitive damages, reasonable attorneys' fees and litigation costs, and Defendants' profits obtained from the violations described above. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiff's remedy at law is not adequate to compensate them for these inflicted and threatened injuries, entitling Plaintiff to remedies, including injunctive relief, as provided by the Wiretap Act.

COUNT III
Computer Fraud and Abuse Act

18 U.S.C. § 1030

61. Plaintiff incorporates the allegations in each above numbered paragraph.

62. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"), regulates fraud and related activity in connection with computers. The CFAA makes it unlawful to intentionally access a computer used for interstate commerce or communication without authorization, or to exceed authorized access to such a computer, and to thereby obtain information from a protected computer. 18 U.S.C. § 1030(a)(2)(C).

63. Plaintiff's mobile devices are protected computers as defined by the CFAA.

64. Defendants violated the CFAA by accessing without authorization (or exceeding authorized access to) information from Plaintiff's protected computers. 18 U.S.C. § 1030(a)(2)(C).

65. Defendants violated the CFAA by (A) knowingly causing the transmission of a program, information, code, or command, and as a result intentionally causing damage to Plaintiff's protected computers; (B) intentionally accessing Plaintiff's protected computers without authorization, and as a result recklessly causing damage; and (C) intentionally accessing Plaintiff's protected computers without authorization, and as a result causing damage and loss. 18 U.S.C. § 1030(a)(5).

66. Plaintiff has suffered damages caused by Defendants' CFAA violations. Defendants' intentional actions impaired the integrity of data and information on Plaintiff's mobile devices, including information concerning Plaintiff's phone calls, text messages, web browsing, location and other activities through the keylogging and data transmission

described above. Plaintiff has suffered loss including violation of their right to privacy and degradation of the performance of their mobile devices.

67. As a result of these injuries, Defendants' conduct has caused a loss to one or more persons during a one-year period aggregating at least $5,000 in value in real economic damages.

68. Wherefore, the Plaintiff seeks damages pursuant to 18 U.S.C. § 1030(g).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for judgment against Defendants as follows:

1. Declarations that the actions of Defendant, as set out above, are unlawful;
2. Appropriate injunctive and equitable relief;
3. Compensatory damages;
4. Punitive damages;
5. Statutory damages;
6. Restitution and/or disgorgement;
7. Costs, disbursements, expenses, and attorneys' fees;
8. Pre- and post-judgment interest, to the extent allowable; and
9. Such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff, hereby demands a trial by jury in the case as to all issues so triable.

RESPECTFULLY SUBMITTED,

JOHNSON & BROWN, P.C.

_/s/Curtis D. Johnson, Jr. _____
CURTIS D. JOHNSON, JR.
Bar No. 015518
11 South Idlewild Street
Memphis, Tennessee 38104
Telephone: (901) 725-7520
Facsimile: (901)725-7570
cjohnson@johnsonandbrownlaw.com

_/s/Florence M. Johnson. _____
FLORENCE M. JOHNSON
Bar No. 015499
11 South Idlewild Street
Memphis, Tennessee 38104
Telephone: (901) 725-7520
Facsimile: (901)725-7570
fjohnson@johnsonandbrownlaw.com